Energy Provider Community of Interest

Build Team and Energy Provider Community Meeting

29 June 2016

Securing Networked Infrastructure for the Energy Sector

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE news
- Current projects
  - Situational Awareness (SA) project update
  - Identity and Access Management (IdAM) project update
- SA Build Team introduction and overview
- Open discussion

NCCoE Out and About:

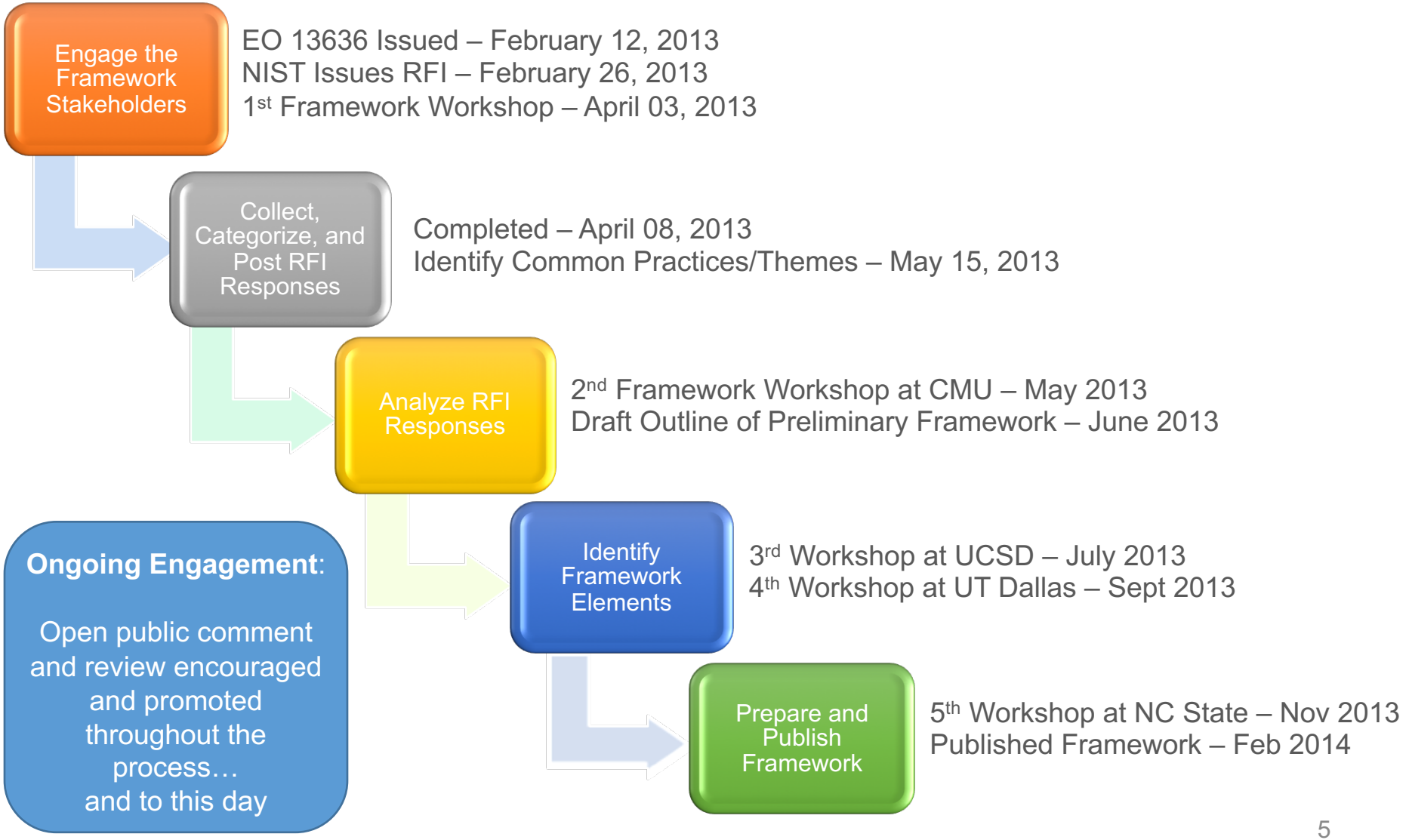
- Attended conferences
  - UTC & Technology (May) – *Nate Lesser spoke*
  - ICS JWG (May) – *Jim McCarthy spoke*
- Upcoming planned conferences
  - APPA National Conference (June)
  - Webinar with AlertEnterprise (June)
  - Cybersecurity for Oil & Gas Summit (June) – *Jim McCarthy speaking*
  - EnergySec (August)
  - Power Grid Cyber Security Exchange (August)
  - ICS Cyber Security Conference Sacramento (October)
  - GridSecCon (October) – *potential workshop*
  - World Congress on Industrial Control Systems Security (WCICSS) (December)

Improving Critical Infrastructure Cybersecurity

- *"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"*

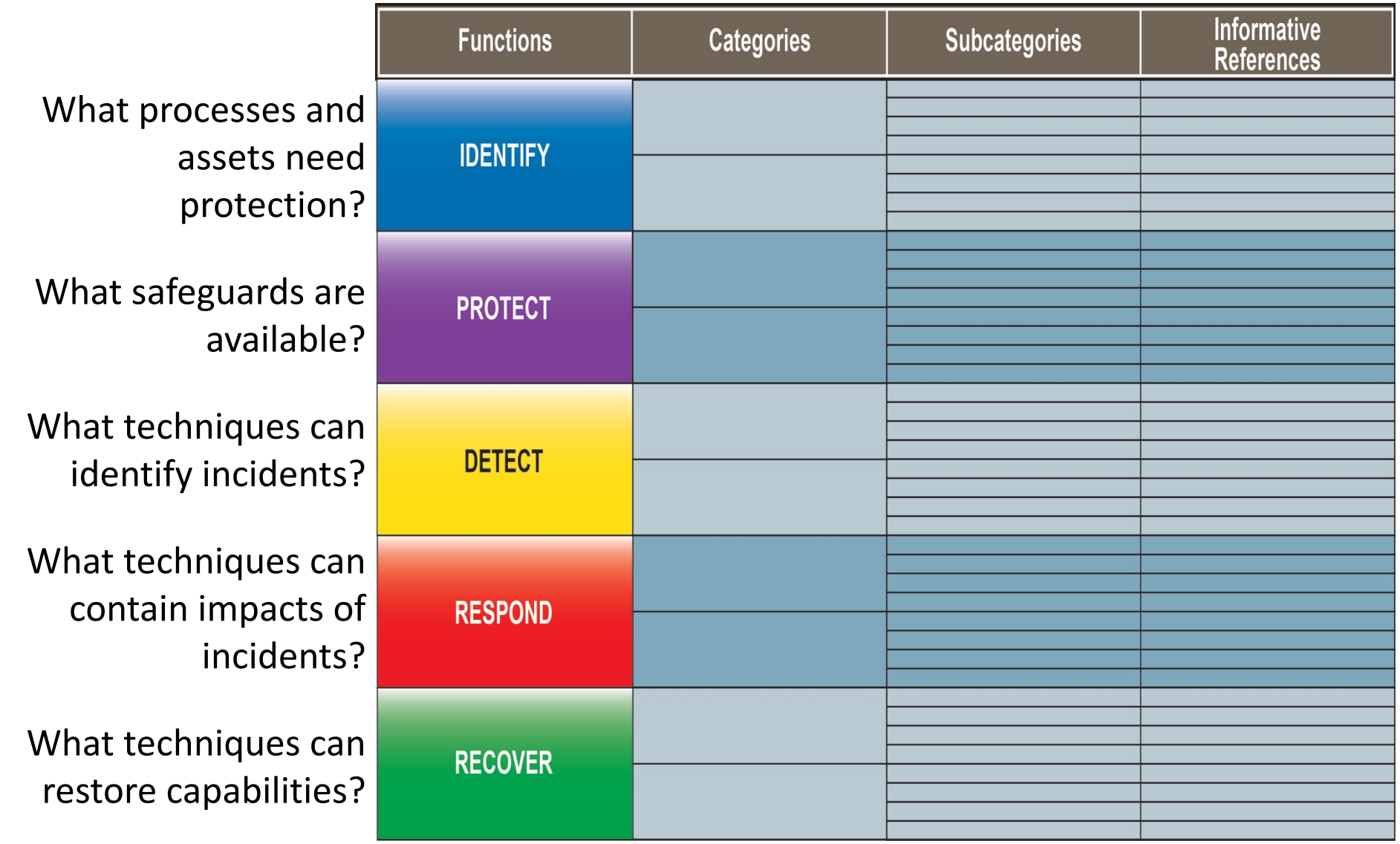
- *President Barack Obama*
- Executive Order 13636, 12 February 2013

Development of the Framework



Framework Core

Cybersecurity Framework Component



Core

Cybersecurity Framework Component

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Exemplar: CSF Mapping for IDAM Reference Solution

Table 1. Use Case Security Characteristics Mapped to Relevant Standards and Controls

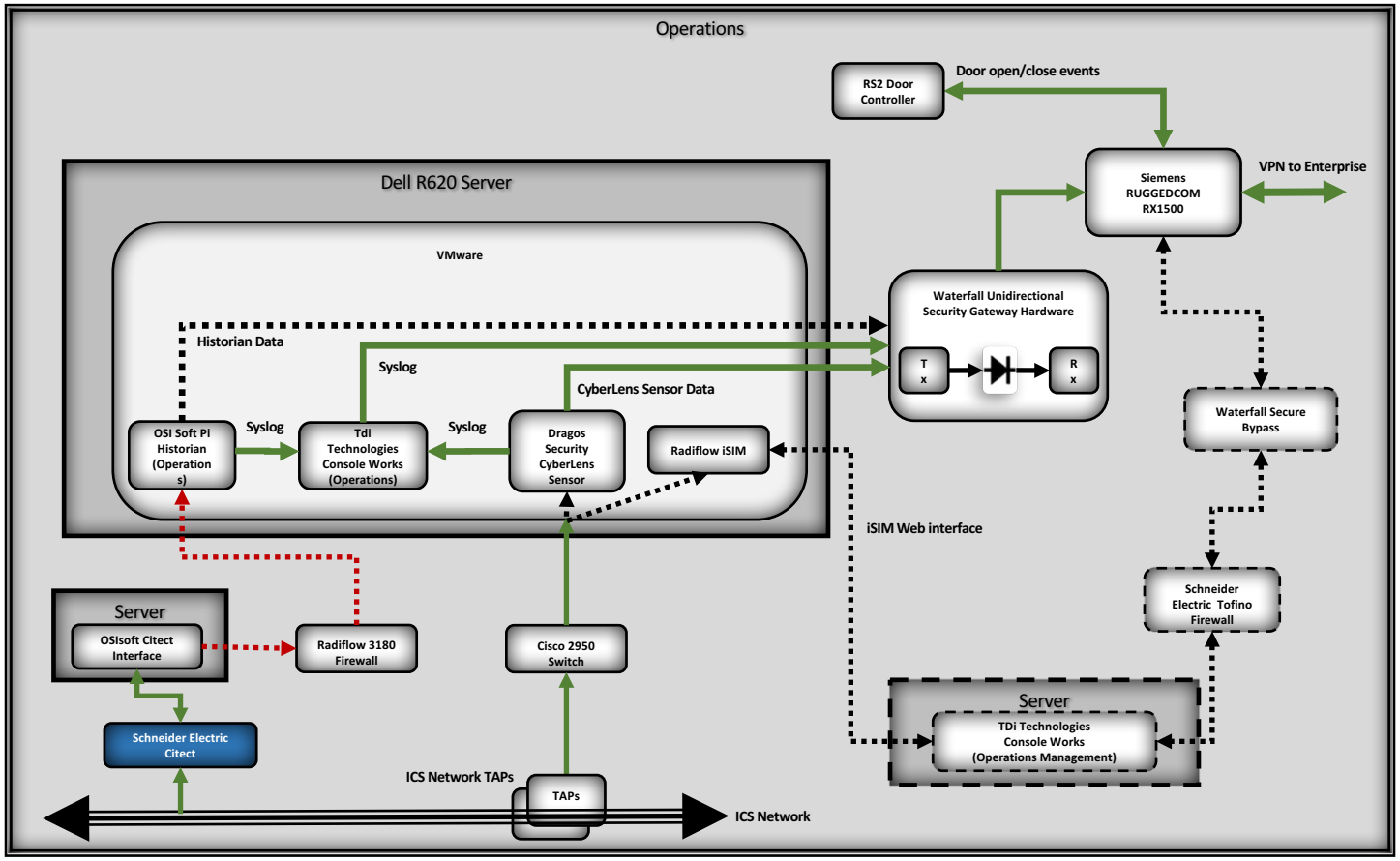
Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC-CIP v.5[1]**
Authentication for OT	Authentication mechanisms	Protect	Access Control	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	AC-2, IA Family	**ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CSC 3-3, CSC 12-1, CSC 12-10,CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-007-5 R2, CIP-007-5 R5

Situational Awareness Project – Installation Update

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MONITORING / DATA COLLECTION BUILD STATUS



Complete

In Process

INSTALLS / INTEGRATIONS COMPLETED

- NCCoE is able to receive data from UMd ICS Network to an OSIsoft Pi historian
- CyberLens Sensor is installed and able to send data through Unidirectional Security Gateway
- ConsoleWorks functioning as a log collector and sending data through Unidirectional Security Gateway
- Network taps are capturing packet data and sending it to Vmware network
  - Not yet sending data to CyberLens or iSID
- Door sensor is sending data over the VPN to RS2 AccessIT!

FINAL TEST CASES

Test Case 1	Event Correlation - OT & PACS: Technician accesses sub-station/control-station and OT device goes down. Alert of anomalous condition and subsequent correlation to PACS to see who accessed facility.
Test Case 2	Event Correlation - OT & IT: Enterprise (IT) java application communication with OT device (Historian) and used as a vector for SQL injection (SQLi)
Test Case 3	Event Correlation - OT & IT / PACS-OT: Unauthorized access attempts detected and alerts triggered based on connection requests from a device on the SCADA network destined for an IP that is outside of the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the Enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.
Test Case 4	Data Exfiltration Attempts: examine behavior of systems; configure SIEM to alert on behavior which is outside the normal baseline. Alerts can be created emanating from OT, IT and PACS. This test case seeks alerting based on behavioral anomalies, rather than recognition of IP addresses.
Test Case 5	Configuration Management: unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. Alert will be created to notify SIEM this has occurred. Detection method will be primarily based on inherent device capability (i.e. log files).
Test Case 6	Rogue Device Detection: alerts are triggered by the introduction of any device onto the ICS network, that has not been registered with the asset management capability in the build.

SA PROJECT MILESTONES

- Use Case published: http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf
- Build team kickoff: 10/20/2015
- Components installed in lab: 12/2015
- Systems integration in new lab: 1/2016 – 3/2016
- Completed build: 05/2016
- Draft Practice Guide release: late June - early July, 2016
- Early adoption: 06/2016 and ongoing
- Demonstrations: 06/2016 and ongoing
- Final Practice Guide release: Fall 2016

DRAGOS SECURITY™

ics²

Hewlett Packard Enterprise

INVOTAS™
ACQUIRED BY FIREEYE

OSIsoft®

radiflow
Secure your Assets

RSA®

RS² Technologies

Schneider Electric

SIEMENS

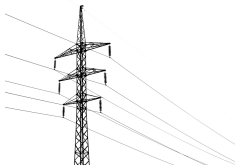
TD

waratek

WATERFALL®
Stronger Than Firewalls

Identity and Access Management (IdAM) Use Case:

Converged management of silos



- Provides a reference solution to:
  - Authenticate individuals and systems
  - Enforce authorization control policies
  - Unify IdAM services
  - Protect generation, transmission and distribution
  - Improve awareness and management of visitor accesses
  - Simplify the reporting process
- Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam
- Final Guide publication pending final approvals
- Demonstrations and adoption support available

IdAM Adoption Activities

- Continue to seek early adoption opportunities
  - *NYPA adoption – projected start is June 2016*
- Collaborating with MITRE for usability study of IdAM Practice Guide
- Opportunities for COI members:
  - Demonstration of solution for your organization
  - Solution feasibility discussions
  - Industry vendor/ integrator introductions
  - COI outreach support

Contact us for more information!

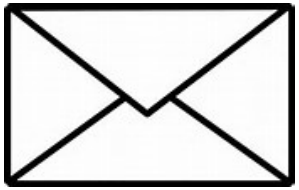
CONTACT US

301-975-0200

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

ABOUT THE NCCOE

National Institute of Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®
Department of Business & Economic Development

MONTGOMERY COUNTY
17 76
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

TENETS

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

PROJECT LIFECYCLE